

## Guidelines for Using Personal Information in Email and Faxes

---

Memorial University employees are required to protect personal information (defined below) from unauthorized access. Appropriate security measures need to be taken whenever handling personal information – your own or someone else’s. Email and faxes, in particular, pose challenges for securing personal information: once you send an email, you’ve lost control of it.

- an emailed message can be copied and forwarded instantaneously to people for whom the message was not intended
- outgoing email may be used by the recipient in a manner beyond your control
- email to and from networks outside the University may not be secure; free webmail accounts in particular (like Yahoo, G-mail, MSN, Hotmail, etc.) are especially vulnerable to masquerading, as no verification of the account holder’s identity occurs at registration
- using “reply to all” may result in unintended, widespread distribution of your message containing personal information
- whether or not in the public domain, email messages are often permanently archived and subject to indexed search and retrieval

These Guidelines are developed in the context of overall University Policy and conform to the requirements of the *Access to Information and Protection of Privacy Act* (“the ATIPP Act”).

## WHAT IS PERSONAL INFORMATION

Personal information is “information about an identifiable individual.” It includes among other things a person’s name, address, telephone number, age, health, financial and educational information, and identifying numbers and symbols like a student number and employee number. This is not an exhaustive list. Any information about an identifiable individual is that person’s personal information. ([Section 2](#))

People’s opinions are also considered to be their personal information. An opinion about another individual, however, is considered to be the personal information of both the opinion-holder and the person the opinion is about. Let’s say you make a complaint to City Hall about your neighbour. The opinion you express is your personal information. However, the opinion is also your neighbour’s personal information, since it is about him. When City Hall responds to your complaint by contacting your neighbour, he may want to know who is making the complaint against him. The tug of war over who owns the personal information is resolved by providing the neighbour with the content of the opinion but not the identity of the person making the complaint.

The University holds personal information belonging to students, faculty, staff, alumni, donors and others. Sometimes personal information may be categorized as *sensitive* personal information. Most often, people consider their health information to be sensitive personal information; others may feel that their personal financial information is particularly sensitive. In terms of privacy risks like unauthorized access, credit card numbers and social insurance numbers are considered to be sensitive personal information.

## EMAIL AND FAXES ARE OFFICIAL RECORDS

Email and faxed transmissions are official records of the University in accordance with University Policy R-2: Records Management. ([Policy R-2](#)) All records you create in carrying out your responsibilities as a University employee are official records, regardless of format.

Nearly all records of the University are subject to the *Access to Information and Protection of Privacy Act* (“the ATIPP Act”) ([the ATIPP Act](#)). That means they are subject to Access to Information requests and those containing personal information are subject to privacy protection requirements. Excluded records under [Section 5](#) include research data and teaching materials.

While sometimes a less formal means of communication, email are nonetheless official records.

## TIPS FOR SENDING EMAIL AND FAXES

- Remember that an emailed message can be copied and forwarded instantaneously to people for whom the message was not intended.
- If you must send sensitive personal information by email, consider sending it as a password-protected Microsoft Office or Adobe Acrobat attachment. Passwords should never be sent by email; they should instead be exchanged in person or over the phone with the intended recipient.

- Explicitly note if a message is confidential and not to be forwarded.
- **Add a confidentiality clause to all your email and faxes.** See the sample below.
- You should not fax or email sensitive personal information unless it is absolutely necessary to send it immediately and faxing or emailing is the only timely way to do so.
- Always use a fax cover sheet, which clearly identifies the sender (with call-back particulars for the sender) and the intended recipient **and contains a confidentiality clause.** See the sample below.
- Before you fax or email personal information, confirm that you have the correct fax number or email address for your intended recipient.
- After you have dialled a fax number, carefully check the number you dialled before sending the fax.
- Do not leave material you have faxed sitting on or near the fax machine. When you are faxing sensitive personal information, stay at the machine during faxing.
- If you must fax sensitive personal information, consider phoning first to ensure that the intended recipient is the right person to receive the fax, the recipient will be there to receive it and to confirm the recipient's fax number. Ask the recipient to call to confirm receipt of the fax.

## CREATING EMAIL AND FAXES

Employees should treat email and faxed transmissions in the same way they would use University letterhead. Create these records with access and privacy protection in mind. As official records of the University, your email may be required in response to a request for information under the ATIPP Act (an ATIPP request) or a systems administrator may be required to produce your email from the server in response to a subpoena ([Policy C-5.2.](#)) Your obligation to protect personal information includes personal information contained in email and faxed correspondence.

- Use caution, common sense and a professional approach.
- Avoid expressing opinions that cannot be supported. As much as possible, stick to the facts and keep it relevant to the subject.
- Be sure that if your email does contain a person's personal information and it is the basis for a decision affecting that person, then you are required to keep the record for at least one year in order to give the individual sufficient opportunity to request access to the information ([Section 37](#)) **(also applies to information you receive).**
- It is recommended that you not include personal information in your email and use non-identifiable terms, if possible.
- Use appropriate business language.

**DISSEMINATION**

- Clearly summarize the contents of your message in the subject line.
- The addresses in the “To” section are for the people you are directly addressing. The addresses in the “CC” section are for the people you are indirectly addressing – copy only those who need to be copied.
- Use “BCC” when addressing a message that will go to a large group of people, or use a mailing list.

**SAMPLE CONFIDENTIALITY NOTICE**

This communication is intended for the use of the recipient to whom it is addressed, and may contain confidential, personal, and/or privileged information. Please contact us immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. Any communication received in error should be deleted or destroyed.